

Data Security

4 th Year Communications

Lecture No. (2)

&

Lecture No. (3)

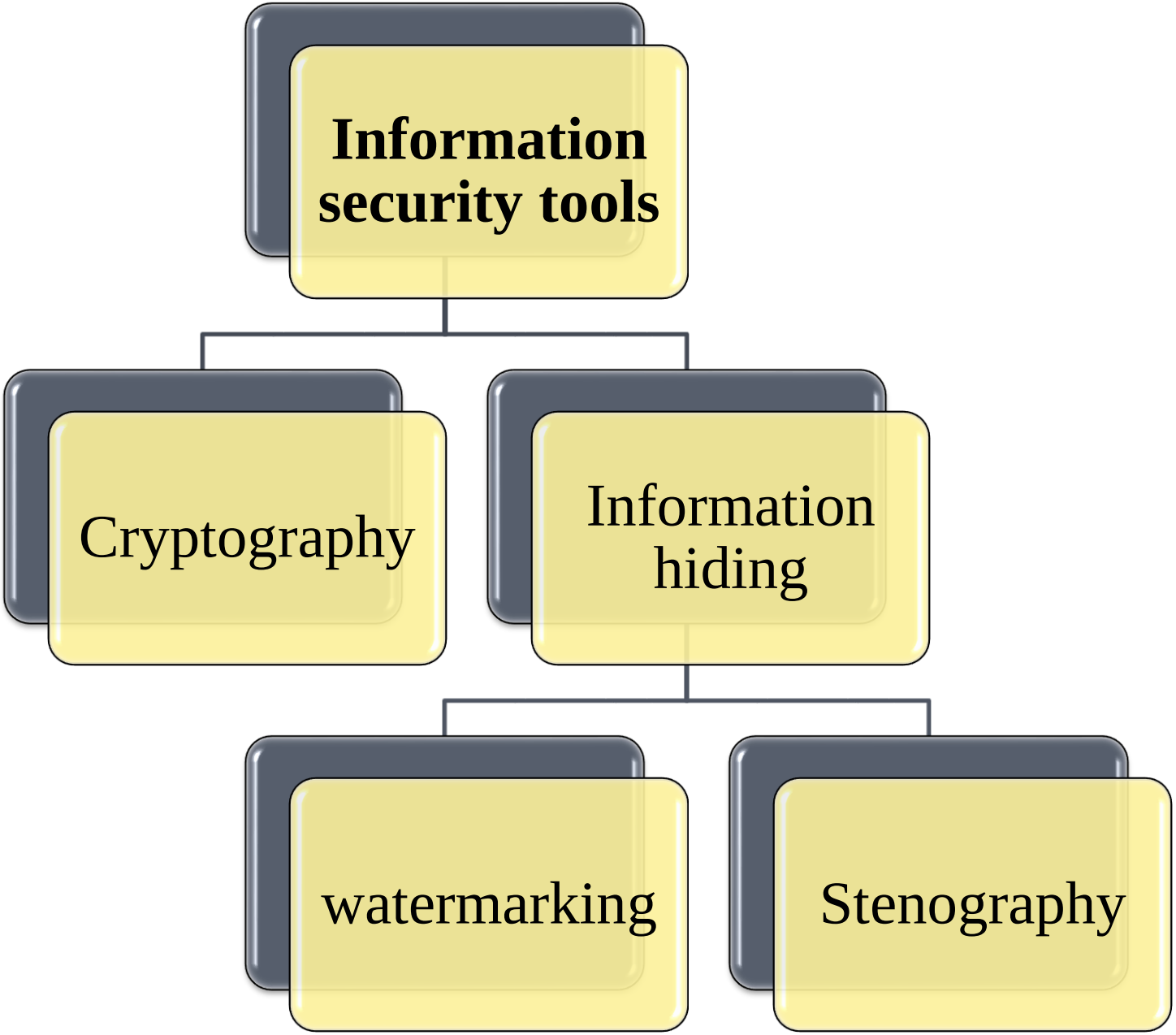
Dr. Roayat Ismail

Learning Objectives

- Discuss Cryptography Terminology
- Discuss Symmetric Key Encryption

Introduction

The actual implementation of security goals needs some help from mathematics. Two techniques are prevalent today: one is very general—*cryptography*—and one is specific—*Information hiding*.


Information security tools
Cryptography
Information hiding
watermarking
Stenography

INFORMATION HIDING :

- Conceal(cover) the existence of message

Cryptography :

- Cryptography, a word with Greek origins, means “secret writing”.

- It means to make the message unintelligible to attackers by encryption

INFORMATION HIDING BRANCHES :

1- Stenography :

- Such as Invisible ink, the word steganography, with its origin in Greek, means “covered writing”.

2- Water marking :

- Used for copy right protection

Cryptanalysis:

A word with Greek origins, *analyein*, meaning “to break up”-is the process of deciphering the original message (or plaintext) from an encrypted message (or ciphertext), without knowing keys used to perform the encryption.

Cryptology:

It includes two disciplines:

Cryptography and Cryptanalysis

Classifications of cryptographic systems :

1- According to the types of operation used to transform plaintext to cipher text . (Substitution & Transposition)

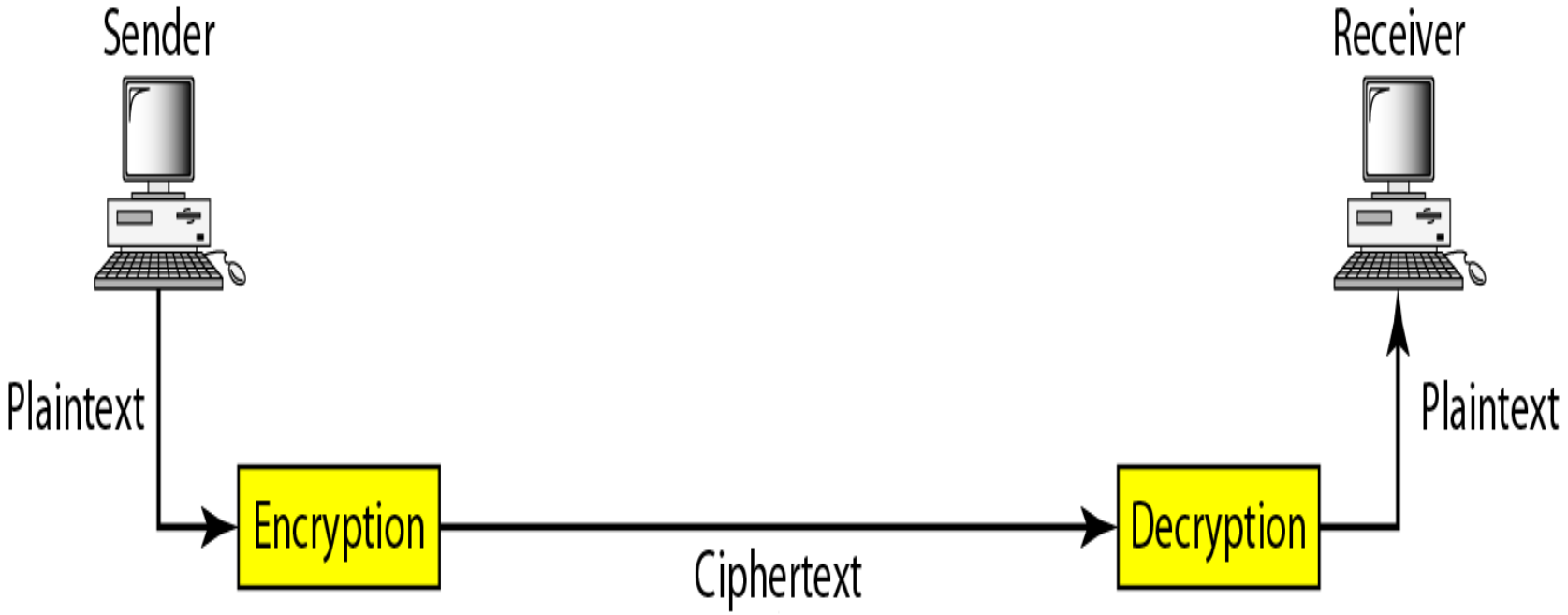
2- According to No. of keys (Symmetric key & Asymmetric key)

3- The way in which the plaintext is processed (block cipher & stream cipher)

Encryption

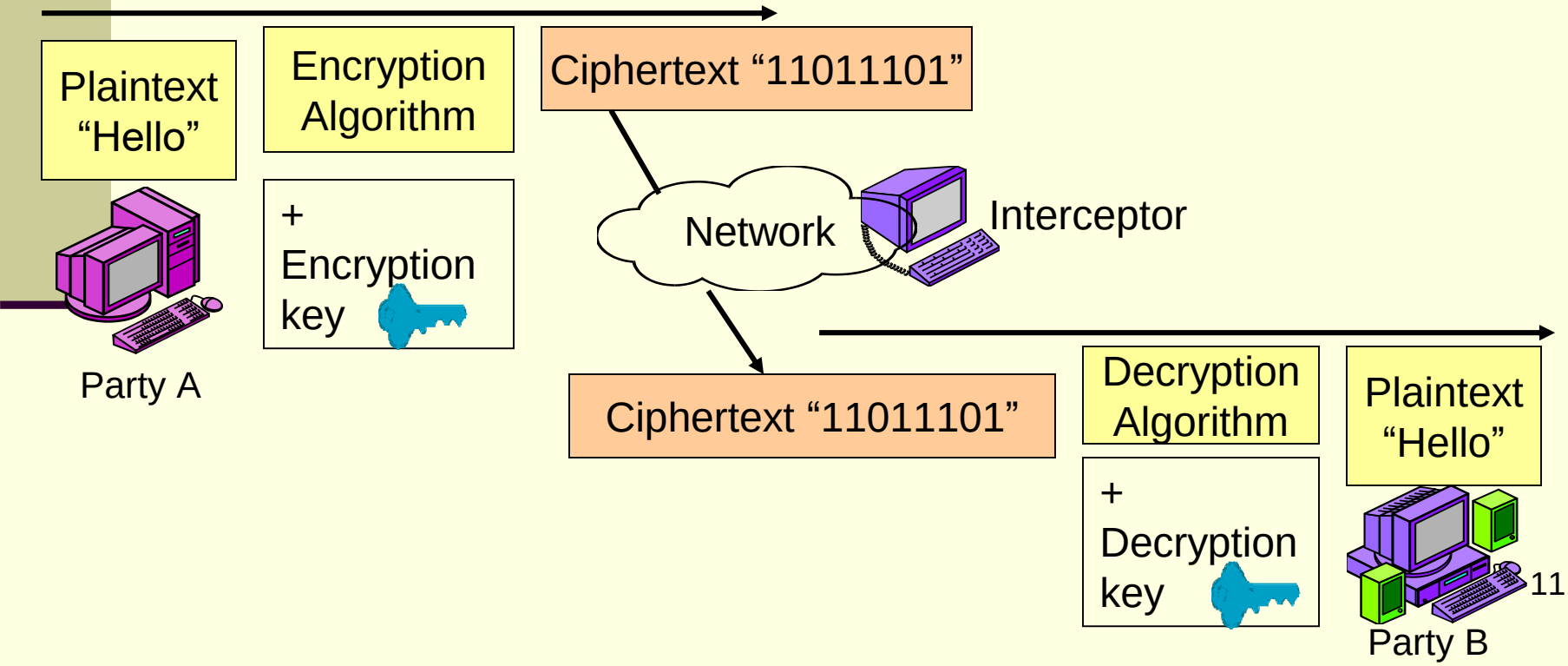
- It is the process of converting an original message into an intelligible form that cannot be used by unauthorized individuals. That way, anyone without the tools and knowledge to convert an encrypted message back to its original format will be unable to interpret.

Figure 30.1 *Cryptography (encryption) components*



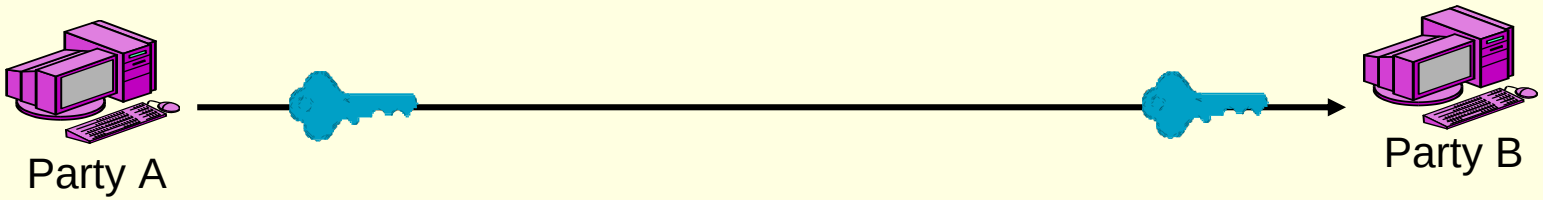
Basic Terminology 1

- **Plaintext:** original message to be sent. Could be text, audio, image, etc.
- **Encryption/Decryption Algorithm:** mathematical tool (software) used to encrypt or decrypt
- **Key:** A string of bits used by to encrypt the plaintext or decrypt the ciphertext
- **Ciphertext:** encrypted message. Looks like a random stream of bits



Basic Terminology 2

- Encryption:
 - Converting plaintext into ciphertext using algorithms and keys
 - The size of the ciphertext is proportional to the size of the plaintext
 - Ciphertext is reversible to plaintext
- Symmetric Key Encryption:
 - Same key is used both for encryption and decryption
 - Keys are identical



- Asymmetric Key Encryption:
 - Also called Public/Private Key Encryption
 - Two different keys are used: one for encryption, one for decryption

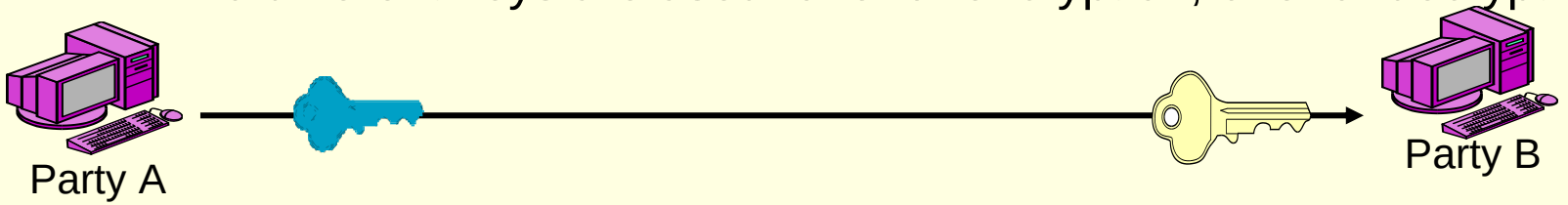
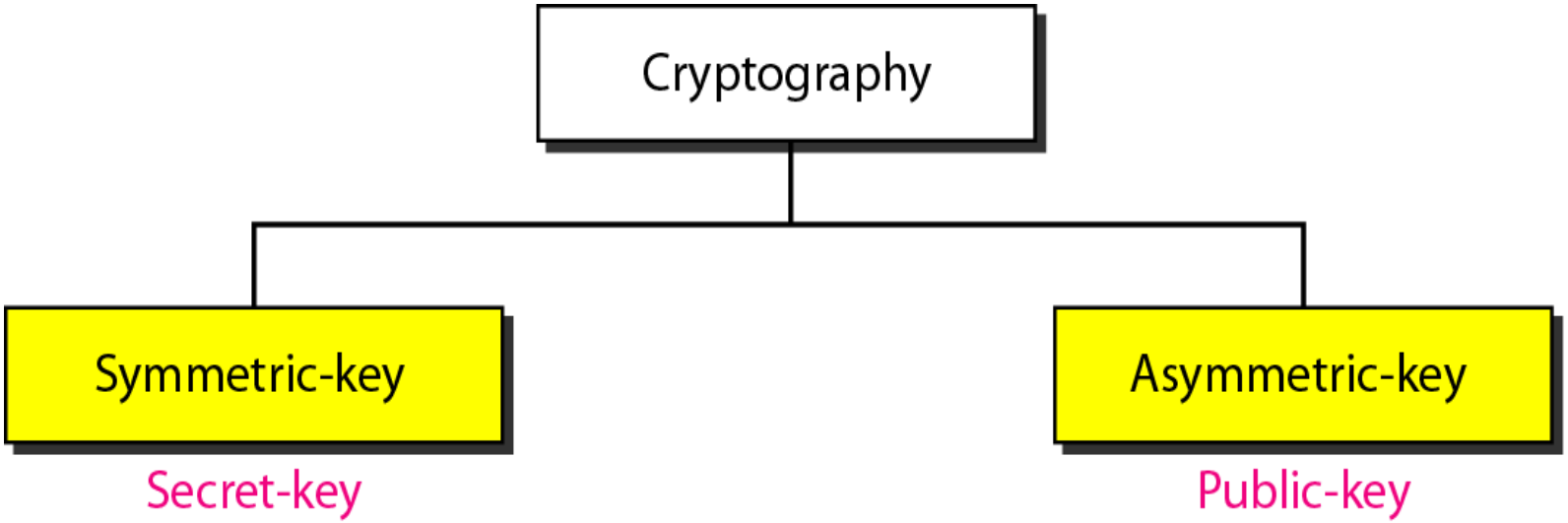


Figure *Categories of cryptography*



Friends and enemies: Alice, Bob, Trudy

- well-known in network security world
- Bob, Alice (lovers!) want to communicate “securely”
- Trudy (intruder) may intercept, delete, add messages

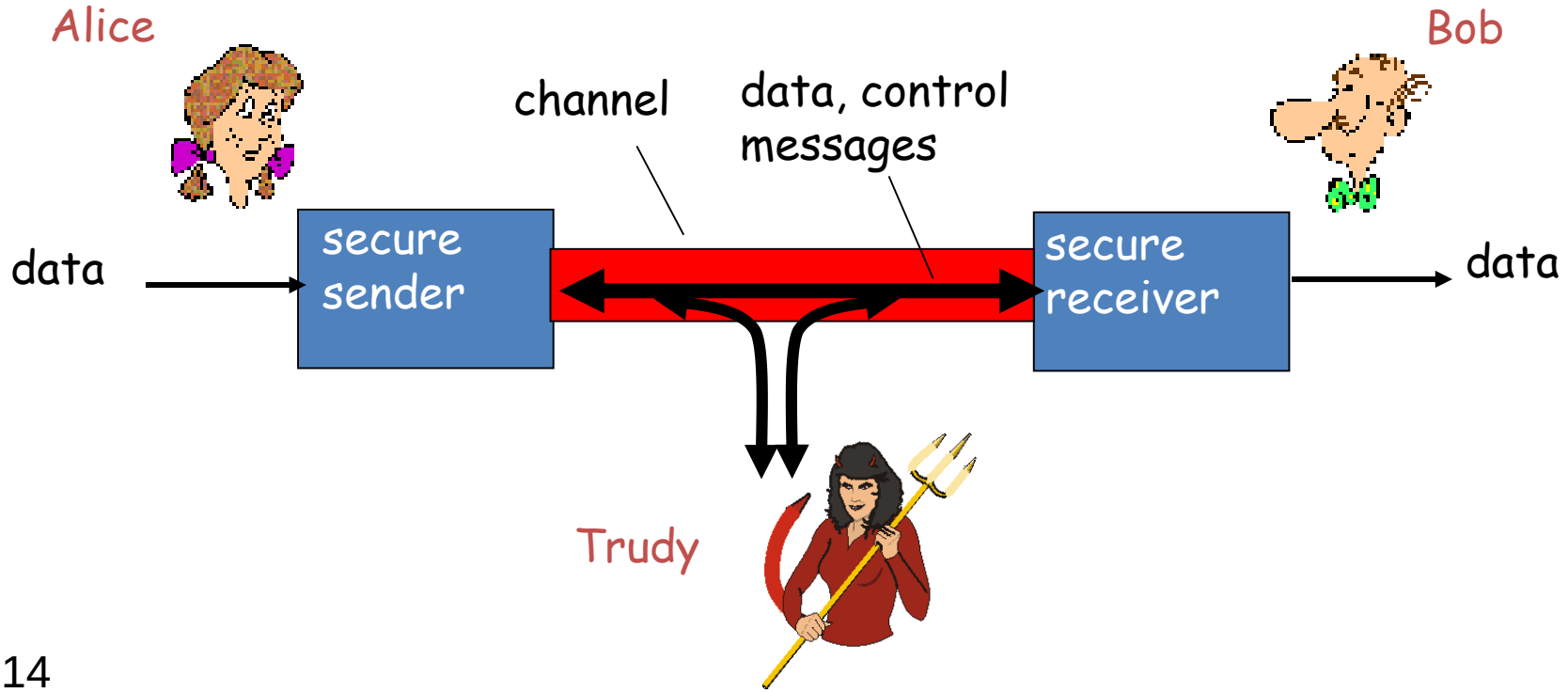
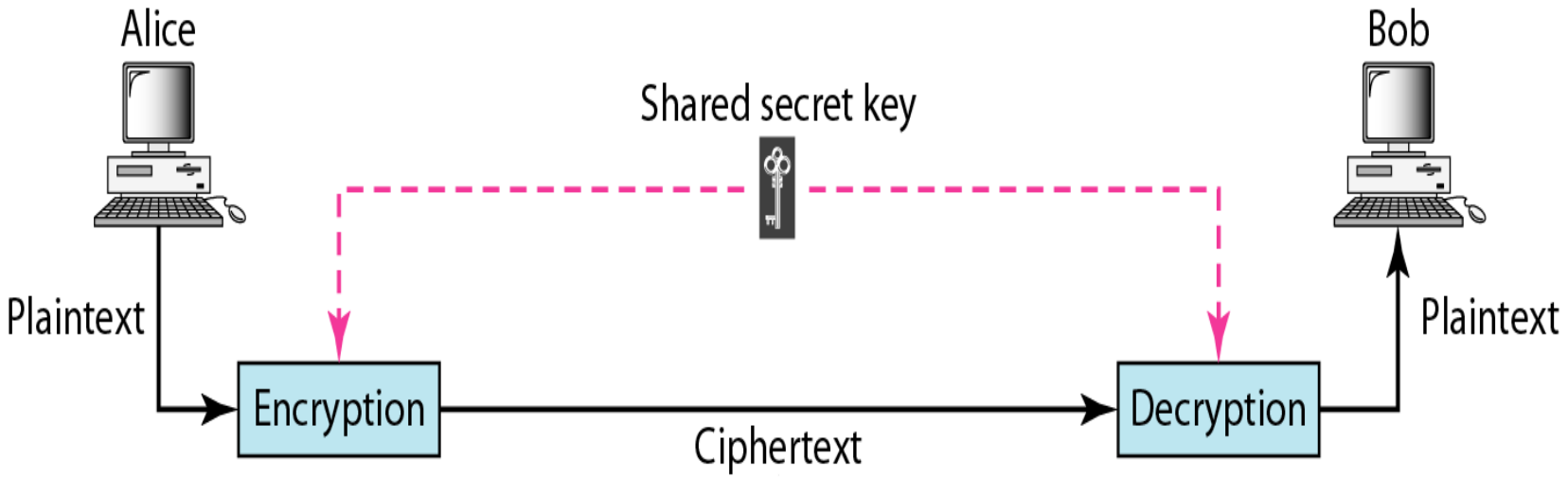


Figure ***Symmetric-key cryptography (conventional cryptography)***



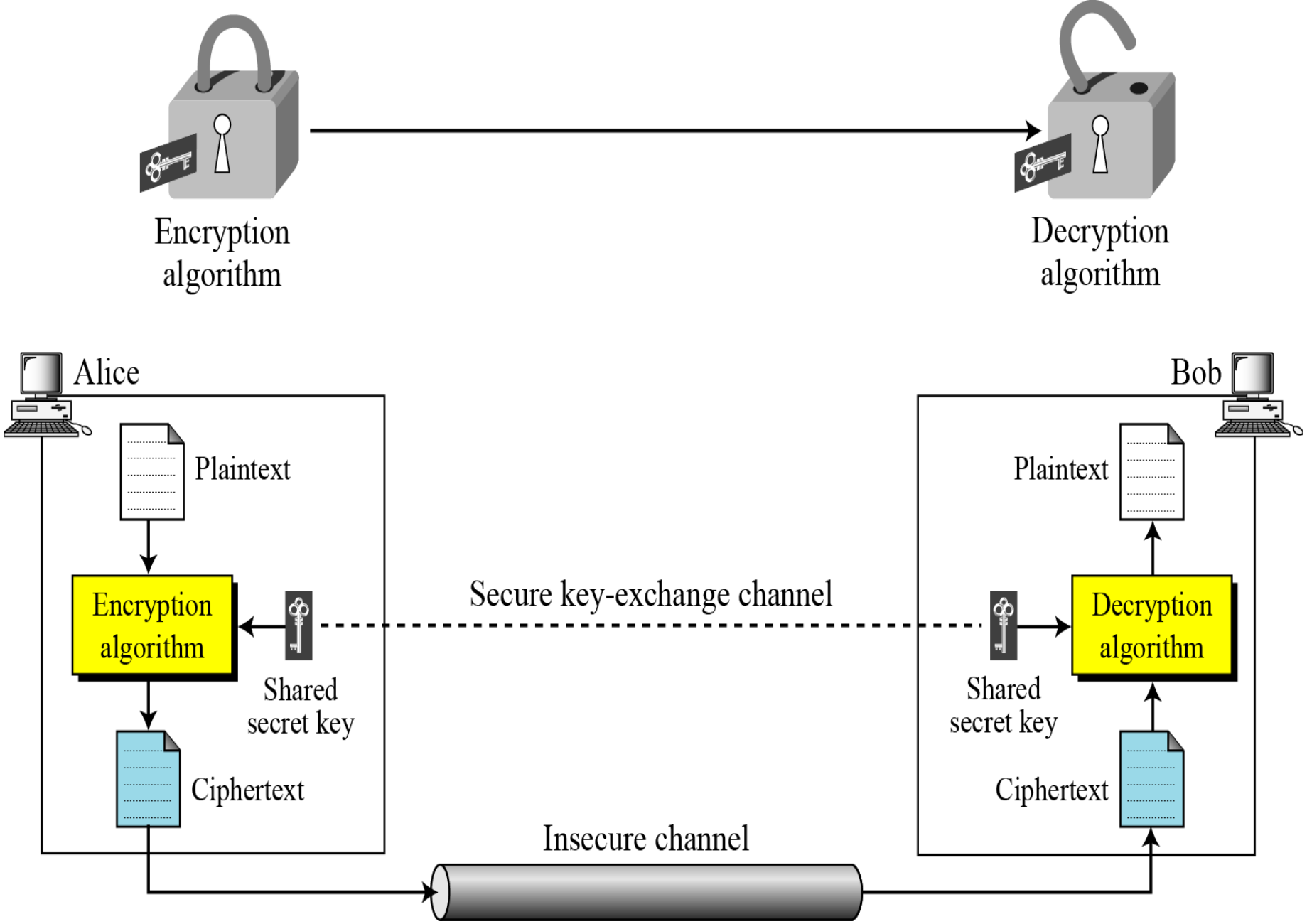
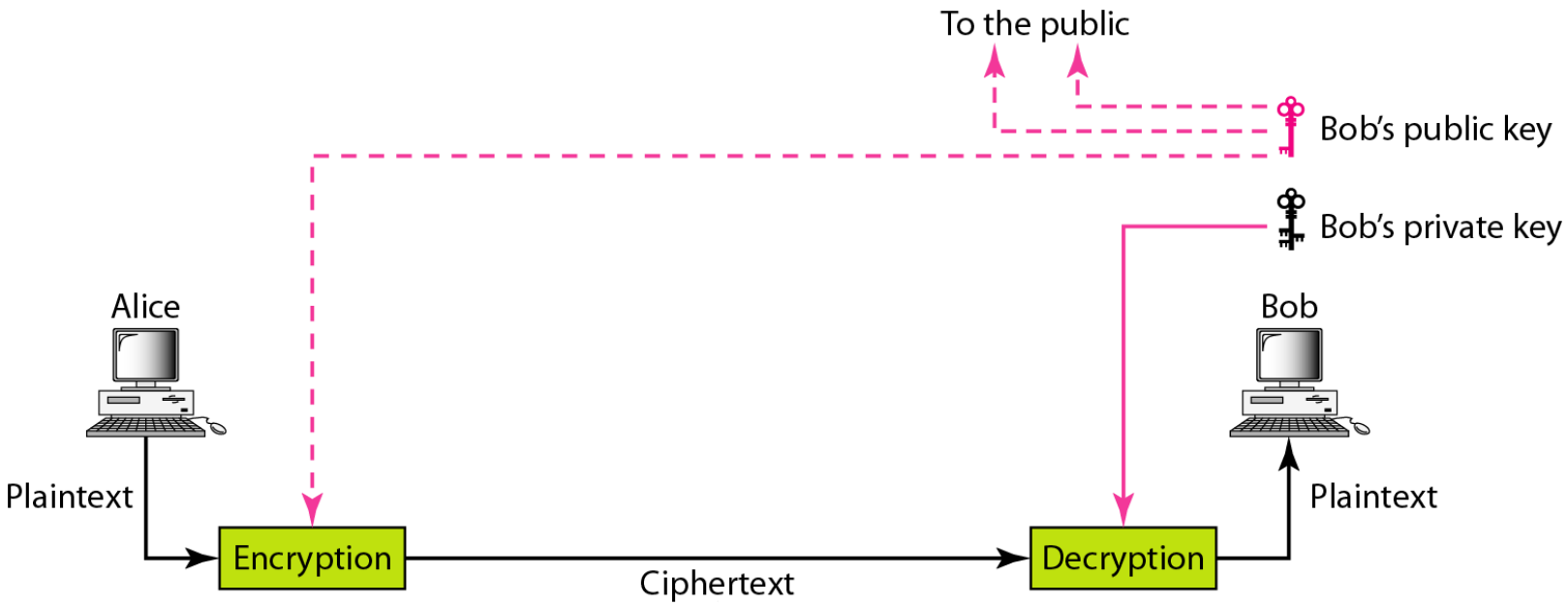


Figure :The general idea of symmetric-key cryptography

Note

In symmetric-key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared.

Figure *Asymmetric-key cryptography (public-key)*



SYMMETRIC-KEY CRYPTOGRAPHY

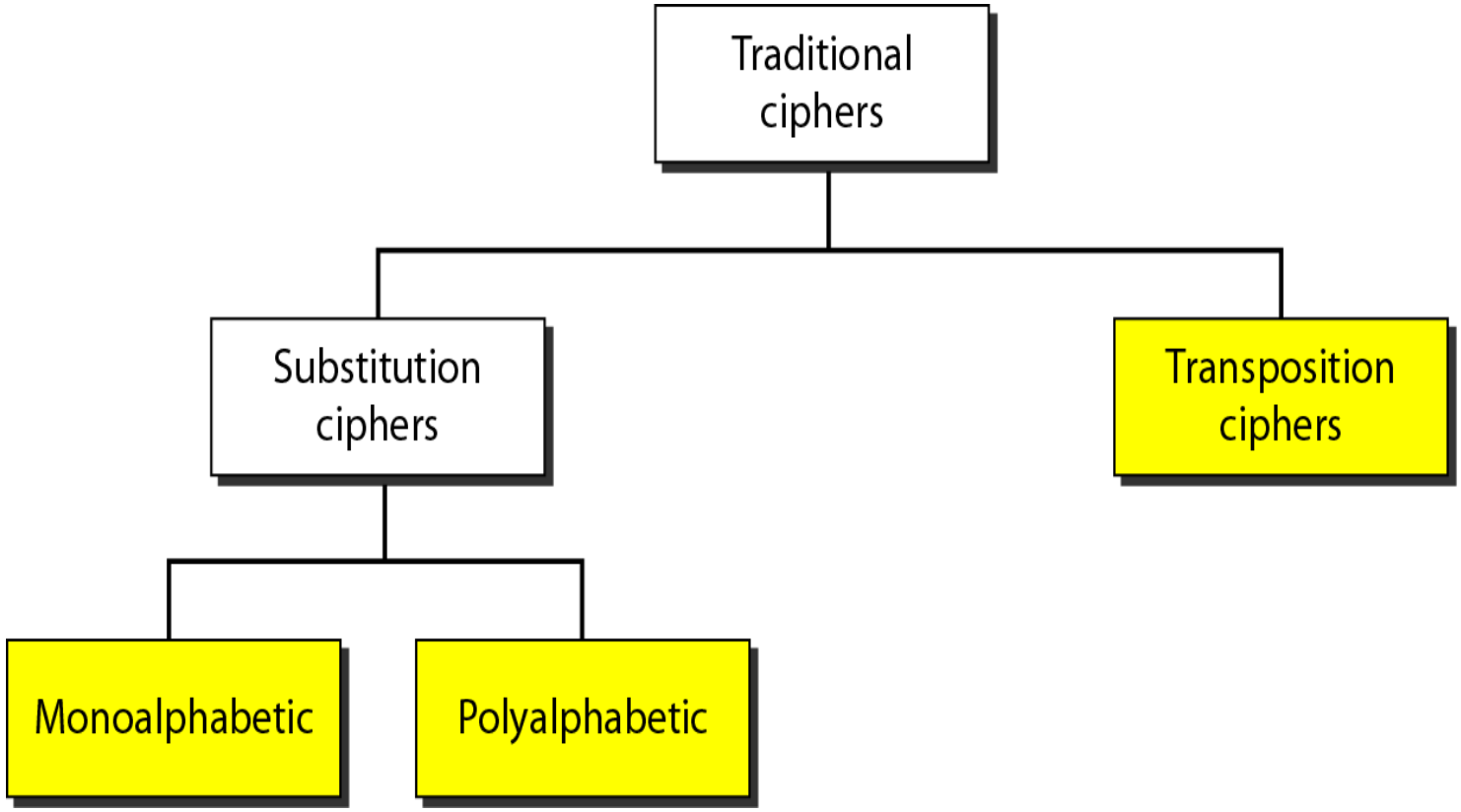
Symmetric-key cryptography started thousands of years ago when people needed to exchange secrets (for example, in a war). We still mainly use symmetric-key cryptography in our network security.

Techniques used for symmetric - key cryptography :

1- Substitution

2- Transposition

Figure *Traditional ciphers*



1- Substitution :

- **Types of Substitution :**

A- Simple substitution or Mono-alphabetic

B- Homophonic cipher

C- poly alphabetic cipher

A- simple substitution :

- **Types of simple substitution :**

1- addition cipher (Caesar cipher or shift cipher)

2- multiplication cipher

3- affine cipher transformation

1-Monoalphabetic:

A substitution cipher replaces one symbol with another. If the symbols in the plaintext are alphabetic characters, we replace one character with another.

Monoalphabetic cipher: A substitution cipher replaces one symbol
with another.

1. Monoalphabetic Ciphers

In mono-alphabetic substitution,

the relationship between a symbol in the plaintext to a symbol in the ciphertext is always one-to-one.

MATHEMATICAL BACKGROUND

1- Given prime number " p "

$$Z_p = \{ 0, 1, 2 \ldots\ldots\ldots\ldots (p-1) \}$$

Φ(p) : Euler's totien function ≡ the number of integers < p and relatively prime (co-prime) with it

Z_p^* = *multiplicative group of p*

EXAMPLE :

Let p= 5

$$Z_p = \{0\ ,1\ ,2\ ,3\ ,4\}$$

$$Z_p^* = \{\ 1\ ,2\ ,3\ ,4\}$$

Φ(5)=(5-1)=4

2- Given composite number : n

- n=p*q

$$z_n = \{ 0 ,1,2,3, \dots \dots \dots \dots \dots . (n-1)\}$$

- if p≠ q then Φ(n)= (p-1)(q-1)

EXAMPLE :

- n=35 = 5*7

$$Z_n = \{0 , 1 , 2 , \ldots\ldots\ldots\ldots\ldots\ldots 34 \}$$

Φ(35)=4*6 =24

FERMAT 'S THEORY :

Given integers a , p

Where : p is prime number

gcd (a , p)=1

$$a^{\Phi(p)} \bmod p \equiv 1$$

EULER 'S THEOREM :

Given integers a , n

Where : n= p * q & p , q are primes

gcd (a , n)=1

$$a^{\Phi(n)} \equiv 1 \mod n$$

$$a^{\Phi(n)-1} \equiv a^{-1} \quad mod n$$ ⇨ a,n co prime

1- shift cipher :

- **Encryption :**

$$C \equiv (P + K) \bmod 26$$

- **Decryption :**

$$P \equiv (C - K) \bmod 26$$

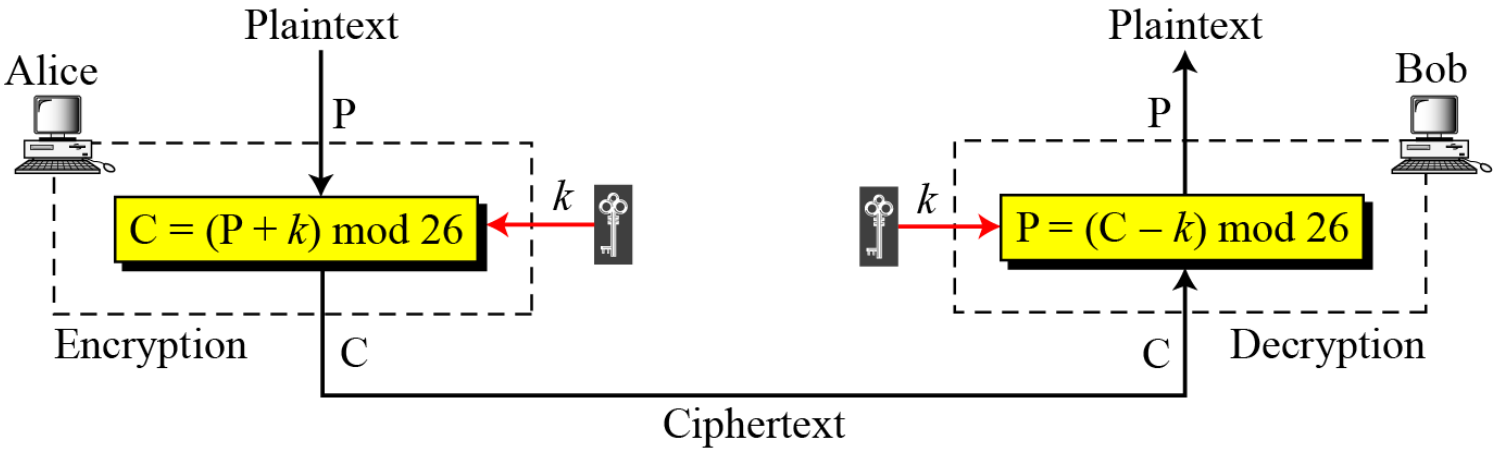
Where :

P : plain text (intelligible text or un-encrypted text)

C: cipher text (unintelligible text or encrypted text)

K : key of cryptographic algorithm

Figure: ***Additive cipher (shift cipher)***



When the cipher is additive,
the plaintext, ciphertext, and key are integers in Z_{26}.

Example1

Use the shift cipher with key = 15 to encrypt the message "HELLO."

Solution

We encrypt one character at a time. Each character is shifted 15 characters "down". Letter H is encrypted to W. Letter E is encrypted to T. The first L is encrypted to A. The second L is also encrypted to A. And O is encrypted to D. The cipher text is WTAAD.

Use the additive cipher with key = 15 to encrypt the message "hello".

Solution

We apply the encryption algorithm to the plaintext, character by character:

Plaintext: h	→	Shift 15 characters down	→	Ciphertext: w
Plaintext: e	→	Shift 15 characters down	→	Ciphertext: t
Plaintext: l	→	Shift 15 characters down	→	Ciphertext: a
Plaintext: l	→	Shift 15 characters down	→	Ciphertext: a
Plaintext: o	→	Shift 15 characters down	→	Ciphertext: d

The ciphertext is therefore "wtaad".

Example 2

Use the shift cipher with key = 15 to decrypt the message "WTAAD."

Solution

We decrypt one character at a time. Each character is shifted 15 characters "up". Letter W is decrypted to H. Letter T is decrypted to E. The first A is decrypted to L. The second A is decrypted to L. And, finally, D is decrypted to O. The plaintext is HELLO.

Ciphertext: W → 22	Decryption: (22 – 15) mod 26	Plaintext: 07 → h
Ciphertext: T → 19	Decryption: (19 – 15) mod 26	Plaintext: 04 → e
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: D → 03	Decryption: (03 – 15) mod 26	Plaintext: 14 → o

Example .3

Caesar cipher: key =3

Substitute message character with the character three values to the right in the alphabet :
Input text:
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Output text:
DEFGHIJKLMNOPQRSTUVWXYZABC

The plaintext: Berlin becomes ehuolq

➢EXAMPLE4

Encrypt : “ meet me after party “

Using key =3

Encrypted message :

PHHW PH DIWHU SDUWB

Example 5.1

The following shows a plaintext and its corresponding ciphertext. The cipher is probably monoalphabetic because both *l*'s (els) are encrypted as *O*'s.

Plaintext: hello **Ciphertext:** KHOOR

Example5.2

The following shows a plaintext and its corresponding ciphertext. The cipher is not monoalphabetic because each *l* (el) is encrypted by a different character.

Plaintext: hello **Ciphertext:** ABNZF

Example 6 (the encryption key can be given as a table):
Use the following key to encrypt the message

this message is easy to encrypt but hard to find the key

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext →																										
Ciphertext →	N	O	A	T	R	B	E	C	F	U	X	D	Q	G	Y	L	K	H	V	I	J	M	P	Z	S	W

The ciphertext is

ICFVQRVVNEFVRNVSIYRGAHSLIOJICNHTIYBFGTICRXRS

2- multiplication cipher :

- **Encryption :**

$$C \equiv (P * K) \bmod 26$$

- **Decryption :**

$$P \equiv (C * K^{-1}) \bmod 26$$

Where : K , n co- prime , n=26

➢EXAMPLE ON MULTIPLICATION CIPHER :

Encrypt : “ tomorrow “

Using k=9

➢Solution :

Cipher : “ PWEWXXWQ “

3- affine cipher transformation :

- **Encryption :**

$$C \equiv (a * P + b) \mod 26$$

- **Decryption :**

$$P \equiv \{(C - b) * a^{-1}\} \mod 26$$

Where : gcd(a , n)=1 , n=26

- **Example on affine cipher transformation :**

Encrypt : “ please send money “

Using a= 7 & b= 10

➢SOLUTION OF PREVIOUS EXAMPLE :

Encrypted message :

“ LJMKGM GMXF QEXMW “

Attacks on Mono-alphabetics :

1- Brute force attack

2- letter frequency distribution



A- single letter frequency distribution

B-two letters (diagram) frequency distribution

Cryptanalysis Monoalphabetic Ciphers

1.Brute-Force Attack :

•Exhaustive-key-search method,

•Attacker has "ciphertext" tries all possible keys until he obtain intelligible plaintext.

2. Frequency Letters Analysis:

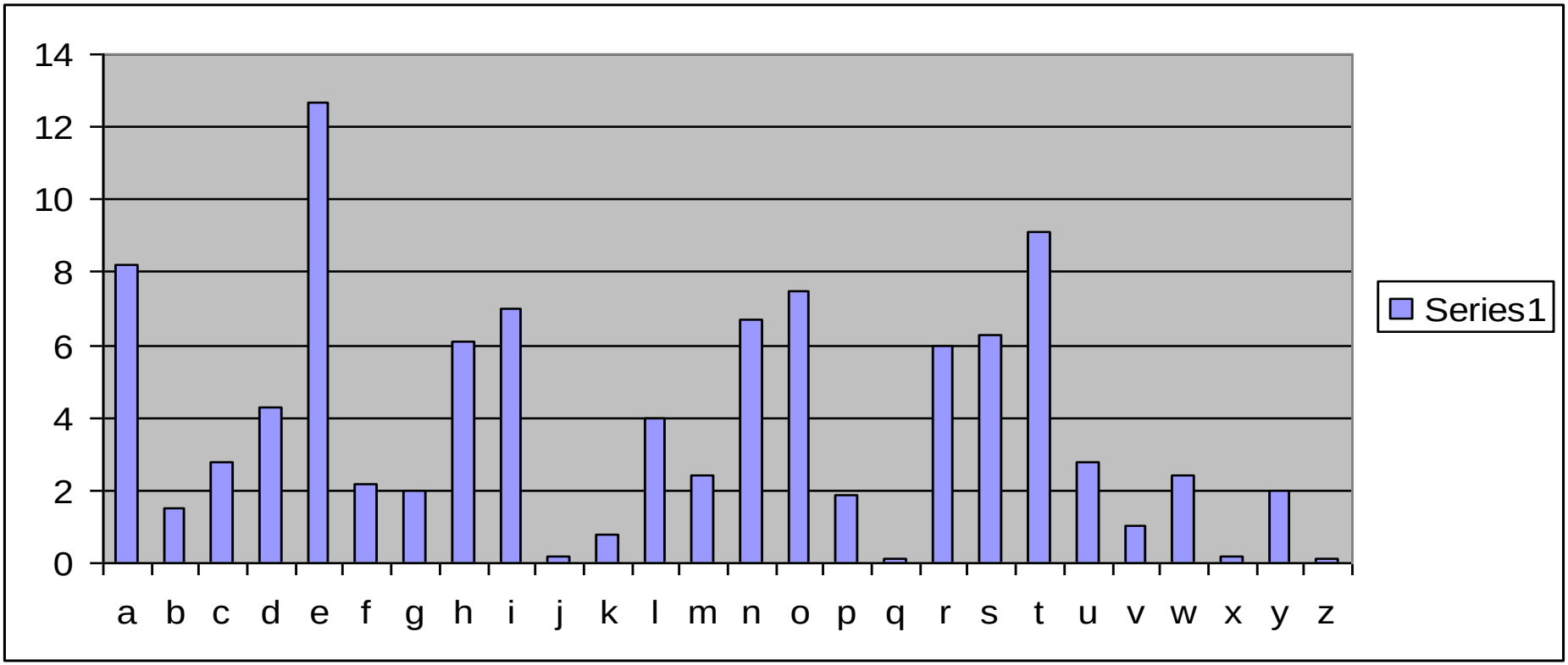
Basic ideas:

Each language has certain features: frequency of letters, or of groups of two or more letters.

Substitution ciphers preserve the language features.

Substitution ciphers are vulnerable to frequency analysis attacks.

Frequency of Letters in English



Frequency Analysis Attack

Table1 *Frequency of characters in English*

Letter	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*
E	12.7	H	6.1	W	2.3	K	0.08
T	9.1	R	6.0	F	2.2	J	0.02
A	8.2	D	4.3	G	2.0	Q	0.01
O	7.5	L	4.0	Y	2.0	X	0.01
I	7.0	C	2.8	P	1.9	Z	0.01
N	6.7	U	2.8	B	1.5		
S	6.3	M	2.4	V	1.0		

Table 2 *Frequency of diagrams and trigrams*

Digram	TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF
Trigram	THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH

Example7

Eve has intercepted the following ciphertext.
Using a statistical attack, find the plaintext.

XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-
VVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW

Solution

When Eve tabulates the frequency of letters in this ciphertext, she gets: **I** =14, **V** =13, **S** =12, and so on.
The most common character is **I** with 14 occurrences.
This means key = 4.

the house is now for sale for four million dollars it is worth more hurry before the seller receives more offers

Example on Brute-force attack

- Can an attacker find K?
 - YES: by a brute-force attack through exhaustive key search,
 - key space is small (25 possible keys).

- Once K is found, very easy to decrypt

Example 8

Eve has intercepted the ciphertext "**UVACLYFZLJBYL**".
Show how she can use a brute-force attack
to break the cipher.

Solution

Eve tries keys from 1 to 7. With a key of 7,
the plaintext is "not very secure", which makes sense.

Ciphertext: UVACLYFZLJBYL

K = 1	→	**Plaintext:** tuzbkxeykiaxk
K = 2	→	**Plaintext:** styajwdxjhzwj
K = 3	→	**Plaintext:** rsxzivcwigyvi
K = 4	→	**Plaintext:** qrwyhubvhfxuh
K = 5	→	**Plaintext:** pqvxgtaugewtg
K = 6	→	**Plaintext:** opuwfsztfdvsf
K = 7	→	**Plaintext:** notverysecure

Disadvantages of Mono-alphabetic

They are easy to break because they reflect the frequency data of the original alphabet. In ciphertext, different letters have different frequency. Each letter in the ciphertext corresponds to only one letter in the plaintext letter.

Idea for a stronger cipher:

Use more than one cipher alphabet, and switch between them when encrypting different letters. As result, frequencies of letters in ciphertext are similar (flat). This can be achieved by using:

1. Homophonic ciphers
2. Polygram
3. Polyalphabetic ciphers

Homophonic substitution :

- It provides multiple substitutes , known as homophones for a single letter

- With each homophone used in rotation or randomly

- If the number of symbols assigned to each letter is proportional to relative frequency of that letter , then single letter frequency information is completely counter measured

- Suppose that English letters are encrypted as integers between 00 to 99

- Where the number of integers assigned to a letter is proportional to relative frequency of that letter

EXAMPLE:

Encrypt the message "plain pilot"

Letter	Homophones								
P	33	91							
L	03	44	76						
A	17	19	34	41	56	60	67	83	
I	08	22	53	65	88	90			
N	02	09	15	27	32	40	59		
O	01	11	23	28	42	54	70	80	
T	05	10	20	29	45	58	64	78	99

One possible encryption of the message:

Pain text	P	L	A	I	N	P	I	L	O	T
Cipher text	91	44	56	65	59	33	08	76	28	78

Poly grams :

Play fair cipher

Hill cipher

Play fair cipher :

- The best known multiple-letter encryption cipher. It treats diagrams in the plaintext as a single units and translates these units into ciphertext diagrams.
- It is based on the use of a 5×5 matrix of letters constructed using a keyword.

Example :

Encrypt " balloon "

Using key = monarchy

- The matrix is constructed by filling in letters of the keyword (minus duplicates) from left to right and from top to bottom. Then filling in the remainder of the matrix with the remaining letters in alphabetic order. (the letter I/J count as one letter.

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

- Encryption: plaintext is encrypted two letters at a time according to the following rules:

1. Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that:

 "balloon" would be treated as "ba lx lo on"

2. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.

Ex: ar is encrypted as RM

3. Two plaintext letters that fall in the same column are each replaced by the letter beneath with top element of the column circularly following the last.

EX: mu is encrypted as CM

4. Otherwise each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter

EX: hs is encrypted as BP

ea is encrypted as IM

So "balloon" is encrypted to " IB SU PM NA "

POLY ALPHABETIC :

Types :

1-periodic keyword

2- auto keyword

3- vername

Polyaphabetic Substitutions

- To increase security, we can change the cipher alphabet as we are enciphering the message.
- A polyalphabetic cipher is a cipher where different substitution alphabets are used for various parts of the plaintext.
- Example : Encipher the even letters according to one scheme and the odd letters to another…

Example : Suppose we use the substitution

Plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	T	Z	A	B	C	D

to encipher the odd letters of a message (first, third, fifth, etc.) and

Plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G

to encipher the even letters of a message (second, fourth, sixth, etc.). Use this scheme to encipher the message “HELLO THERE HENRY” and comment on why this cipher is no longer monoalphabetic.

Solution: Using the first table for odd letters and the second table for even letters, we obtain

H	**E**	**L**	**L**	**O**	**T**	**H**	**E**	**R**	**E**	**H**	**E**	**N**	**R**	**Y**
L	**L**	**P**	**S**	**S**	**A**	**L**	**L**	**V**	**L**	**L**	**L**	**R**	**Y**	**C**

Vigenere Cipher (Periodic cipher)

Feature:

- It is a periodic substitution cipher based on shift cipher.
- A key word is used to determine which particular rule is chosen for a given transformation.

Example: encrypt the word “renaissance” with a key word “band”.

Plaintext:	R	E	N	A	I	S	S	A	N	C	E	
Key:	B	A	N	D	B	A	N	D	B	A	N	
Ciphertext:	S	E	A	D	Z	W	F	A	V	U	W	

Vigenere Cipher (Auto-key cipher)

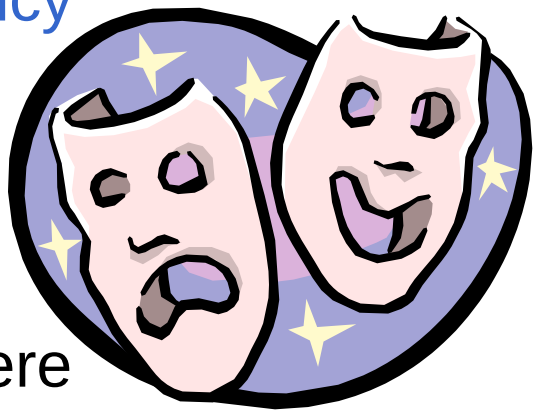
- Non-repeating keyword that is as long as the message itself.
- A keyword is concatenated with the plaintext itself to provide a running key:
- Plaintext: r e n a i s s a n c e
- Key: b a n d r e n a i s s
- Ciphertext: S E A D Z W F A V U W

Vigenere Tableau

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	v	v	w	x	y	z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Security of Vigenere Cipher

- Vigenere masks the frequency with which a character appears in a language: one letter in the plaintext corresponds to multiple letters in the ciphertext. Makes the use of frequency analysis more difficult.
- Any message encrypted by a Vigenere cipher is a collection of as many shift ciphers as there are letters in the key.



Example : Suppose we encipher the message "DOGS" using the keyword "PETS" with the Vigenere cipher square:

Plaintext	**D**	**O**	**G**	**S**
Keyword	**P**	**E**	**T**	**S**
Ciphertext	**S**	**S**	**Z**	**K**

The ciphertext "SSZK" can be obtained mathematically using the MOD 26 alphabet table as follows:

1st Letter: $D \Rightarrow 3$, $P \Rightarrow 15$ $\therefore (3+15)\ MOD\ 26 = 18\ MOD\ 26 = 18 \Rightarrow S$

2nd Letter: $O \Rightarrow 14$, $E \Rightarrow 4$ $\therefore (14+4)\ MOD\ 26 = 18\ MOD\ 26 = 18 \Rightarrow S$

3rd Letter: $G \Rightarrow 6$, $T \Rightarrow 19$ $\therefore (6+19)\ MOD\ 26 = 25\ MOD\ 26 = 25 \Rightarrow Z$

4th Letter: $S \Rightarrow 18$, $S \Rightarrow 18$ $\therefore (18+18)\ MOD\ 26 = 36\ MOD\ 26 = 10 \Rightarrow K$



Example

Let us see how we can encrypt the message "She is listening" using the 6-character keyword "PASCAL". The initial key stream is (15, 0, 18, 2, 0, 11). The key stream is the repetition of this initial key stream (as many times as needed).

Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P's values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	*15*	*00*	*18*	*02*	*00*	*11*	*15*	*00*	*18*	*02*	*00*	*11*	*15*	*00*
C's values:	**07**	**07**	**22**	**10**	**18**	**22**	**23**	**18**	**11**	**6**	**13**	**19**	**02**	**06**
Ciphertext:	**H**	**H**	**W**	**K**	**S**	**W**	**X**	**S**	**L**	**G**	**N**	**T**	**C**	**G**

VERNAM :

- It uses a keyword that is as long as the plaintext and has no statistical relationship to it.
- It works on binary data.
- A binary message: $m_1, m_2, \ldots\ldots, m_t$
- A binary key string: $k_1, k_2, \ldots\ldots, k_t$ the same length.
- The ciphertext string:

$C_1, C_2, \ldots\ldots, C_t$ where:

$$C_i = m_i \text{ XOR } k_i$$

If the key string is randomly chosen and never used again this cipher is called one-time-pad.

Transposition :

Types :

1- Rail fence transposition

2- Columnar transposition

3- Periodic transposition

7. TRANSPOSITION CIPHERS

A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols.

A transposition cipher reorders symbols.

It has two types:

1. Keyed Transposition Ciphers
2. Keyless Transposition Ciphers

Keyless Transposition Ciphers

Simple transposition ciphers,
which were used in the past, are keyless.

1. Text is written into a table column by column and then is transmitted row by row.

2. Text is written into a table and row by row then is transmitted column by column.

Keyless Transposition Ciphers

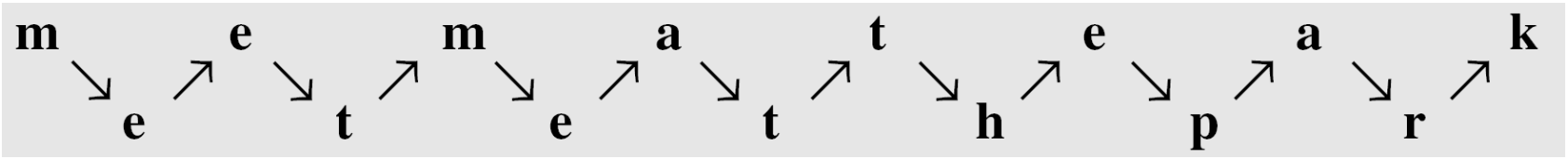
Example

A good example of a keyless cipher using the first method is the rail fence cipher.

The ciphertext is created reading the pattern row by row.

For example,

to send the message "**Meet me at the park**" to Bob, Alice writes



She then creates the ciphertext "**MEMATEAKETETHPR**".

Keyless Transposition Ciphers (cont.)

Example

Alice and Bob can agree on the number of columns and use the second method.

Alice writes the same plaintext, row by row, in a table of four columns.

m	e	e	t
m	e	a	t
t	h	e	p
a	r	k	

She then creates the ciphertext "**MMTAEEHREAEKTTP**".

Keyed Transposition Ciphers

The keyless ciphers permute the characters by using writing plaintext in one way and reading it in another way.

The permutation is done on the whole plaintext to create the whole ciphertext.

Another method is to divide the plaintext into groups of predetermined size, called blocks, and then use a key to permute the characters in each block separately.

Keyed Transposition Ciphers (cont.)

Example

Alice needs to send the message "Enemy attacks tonight" to Bob.

e n e m y a t t a c k s t o n i g h t z

The key used for encryption and decryption is a permutation key, which shows how the characters are permuted.

Encryption ↓

3	1	4	5	2
1	2	3	4	5

↑ Decryption

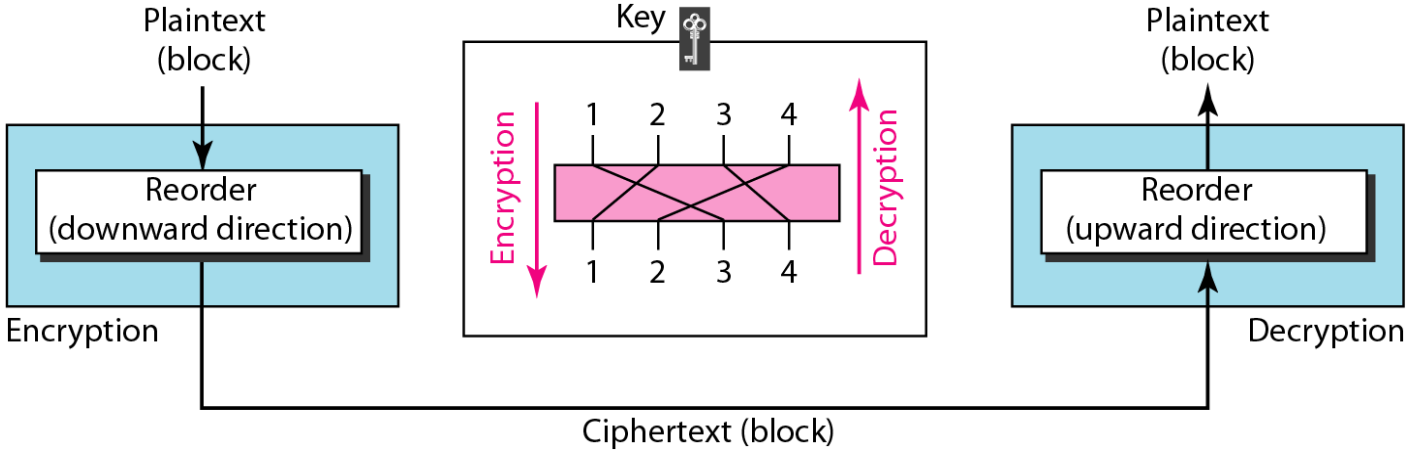
The permutation yields

E E M Y N T A A C T T K O N S H I T Z G

Note

A transposition cipher reorders (permutes) symbols in a block of symbols

Figure *Transposition cipher*



Example

Encrypt the message "HELLO MY DEAR," using the key shown in the previous figure.

Solution

We first remove the spaces in the message. We then divide the text into blocks of four characters. We add a bogus character Z at the end of the third block. The result is HELL OMYD EARZ. We create a three-block ciphertext ELHLMDOYAZER.

Example

Using the previous Example , decrypt the message "ELHLMDOYAZER".

Solution

The result is HELL OMYD EARZ. After removing the bogus character and combining the characters, we get the original message "HELLO MY DEAR."